ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0013—2021
代替 GM/T 0013—2012

可信计算　可信密码模块接口符合性测试规范

Trust computing—Trusted cryptography module interface compliance

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅴ
引言 …… Ⅶ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　可信密码模块接口符合性测试 …… 2
4.1　概述 …… 2
4.2　常量值 …… 3
4.3　测试策略 …… 4
4.4　测试方法 …… 5
5　命令依赖关系 …… 6
5.1　概述 …… 6
5.2　启动命令集 …… 6
5.3　状态保存命令集 …… 6
5.4　自检命令集 …… 6
5.5　TCM 工作模式设置命令集 …… 7
5.6　Owner 管理命令集 …… 7
5.7　属性管理命令集 …… 7
5.8　升级与维护命令集 …… 7
5.9　授权值管理命令集 …… 7
5.10　非易失存储管理命令集 …… 7
5.11　运行环境管理命令集 …… 8
5.12　审计命令集 …… 8
5.13　时钟命令集 …… 8
5.14　计数器命令集 …… 8
5.15　TCM 背书密钥管理命令集 …… 9
5.16　平台身份密钥管理命令集 …… 9
5.17　数据保护操作命令集 …… 9
5.18　密钥管理命令集 …… 10
5.19　密钥协商命令集 …… 10
5.20　密钥迁移命令集 …… 10
5.21　密码服务命令集 …… 11
5.22　传输会话命令集 …… 11
5.23　授权协议命令集 …… 12
5.24　平台配置寄存器管理命令集 …… 12
6　向量命令 …… 12

6.1 概述 …… 12
6.2 TCM_Startup …… 12
6.3 TCM_SelfTestFull …… 13
6.4 TCM_ContinueSelfTest …… 14
6.5 TCM_GetTestResult …… 14
6.6 TCM_SetOwnerInstall …… 15
6.7 TCM_OwnerSetDisable …… 15
6.8 TCM_PhysicalEnable …… 17
6.9 TCM_PhysicalDisable …… 17
6.10 TCM_SetTempDeactivated …… 18
6.11 TCM_PhysicalSetDeactivated …… 18
6.12 TCM_TakeOwnership …… 19
6.13 TCM_OwnerClear …… 22
6.14 TCM_ForceClear …… 23
6.15 TCM_DisableOwnerClear …… 24
6.16 TCM_DisableForceClear …… 25
6.17 TCM_GetCapability …… 26
6.18 TCM_SetCapability …… 26
6.19 TCM_ResetLockValue …… 27
6.20 TCM_ChangeAuth …… 29
6.21 TCM_ChangeAuthOwner …… 31
6.22 TCM_NV_DefineSpace …… 32
6.23 TCM_NV_WriteValue …… 35
6.24 TCM_NV_ReadValue …… 35
6.25 TCM_FlushSpecific …… 36
6.26 TCM_GetAuditDigest …… 37
6.27 TCM_GetAuditDigestSigned …… 38
6.28 TCM_SetOrdinalAuditStatus …… 40
6.29 TCM_GetTicks …… 41
6.30 TCM_TickStampBlob …… 42
6.31 TCM_ReadPubEK …… 43
6.32 TCM_OwnerReadInternalPub …… 44
6.33 TCM_MakeIdentity …… 46
6.34 TCM_ActivatePEKCert …… 50
6.35 TCM_ActivatePEK …… 51
6.36 TCM_Seal …… 53
6.37 TCM_Unseal …… 56
6.38 TCM_CreateWrapKey …… 59
6.39 TCM_LoadKey …… 61
6.40 TCM_GetPubKey …… 64
6.41 TCM_CertifyKey …… 65
6.42 TCM_WrapKey …… 67
6.43 TCM_AuthorizeMigrationKey …… 70

6.44 TCM_CreateMigratedBlob …… 71
6.45 TCM_ConvertMigratedBlob …… 74
6.46 TCM_SCHStart …… 77
6.47 TCM_SCHUpdate …… 78
6.48 TCM_SCHComplete …… 78
6.49 TCM_SCHCompleteExtend …… 79
6.50 TCM_Sign …… 80
6.51 TCM_SMS4Encrypt …… 82
6.52 TCM_EccDecrypt …… 84
6.53 TCM_APTerminate …… 86
6.54 TCM_SMS4Decrypt …… 87
6.55 TCM_GetRandom …… 89
6.56 TCM_APCreate …… 90
6.57 TCM_Extend …… 91
6.58 TCM_PCRRead …… 92
6.59 TCM_Quote …… 93
6.60 TCM_PCR_Reset …… 95
7 脚本向量 …… 96
7.1 TCM_SaveState …… 96
7.2 TCM_SaveContext …… 96
7.3 TCM_LoadContext …… 99
7.4 TCM_FiledUpgrade …… 101
参考文献 …… 102

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件代替GM/T 0013—2012《可信计算　可信密码模块接口符合性测试规范》,与GB/T 0013—2012相比主要技术变化如下:

——修订了标准范围描述,修改了“本文件以《可信计算　可信密码支撑平台功能与接口规范》(GM/T 0011—2012)为基础,规范了可信密码模块的接口命令测试向量、测试方法与测试脚本。”(见第1章);

——在规范性引用文件中,删除了“GM/T 0002—2012　SM4分组密码算法 GM/T 0003—2012　SM2椭圆曲线公钥密码算法 GM/T 0004—2012　SM3密码杂凑算法”,修订了“GB/T 32907　信息安全技术　SM4分组密码算法 GB/T 32905　信息安全技术　SM3密码杂凑算法 GB/T 32918(所有部分)　信息安全技术　SM2椭圆曲线公钥密码算法”,修改了“GM/T 0012—2012　可信计算　可信密码模块接口规范　GM/T 0011—2012　可信计算　密码支撑平台功能与接口规范”(见第2章);

——修改了“本文件采用GB/T 32905 GM/T 0004—2012规范标准提供的SM3杂凑算法生成消息验证码。”(见3.6);

——修改了“GM/T 0011—2012定义了可信密码模块(TCM)的设计。”“结构和命令与GM/T 0011—2012的一致性”“本文件仅用于评估可信密码模块与GM/T 0011—2012的符合性”“其中涉及的命令均来自标准GM/T 0011—2012”(见4.1);

——修改了“TCM采用GB/T 32918规范标准提供的SM2非对称密钥算法,TCM采用GB/T 32907规范标准提供的SM4对称密钥算法。”(见4.2.1);

——修改了“TCM采用GB/T 32907标准提供的SM4对称密钥算法”。本文件采用了一个命名的SM4密钥。keyE:用于执行SM4加解密操作。由TCM内部产生。另,在TCM中,SMK也是一个SM4密钥,它具有固定的句柄为40 00 00 00。”(见4.2.1);

——修改了“对TCM产品与GM/T 0011—2012的符合程度进行测试。”“只能通过测试命令的输入和输出来检验是否符合GM/T 0011—2012”(见4.3);

——修改了“则是通过分析GM/T 0011—2012中命令的多种授权方式获得。”(见4.4);

——修改了“由于命令依赖关系繁多复杂,本文件对TCM命令的分类见GM/T 0011—2012”(见第5章);

——修改了“也可以是其他值,参见GM/T 0011—2012中TCM_CAPABILITY_AREA的描述”,“也可以是其他GM/T 0011—2012描述的允许设置的子属性。”(见6.17);

——修改了“c)输出域授权数据验证码的计算过程,参见GM/T 0011—2012的描述。”(见6.33);

——修改了“创建的新密钥的使用授权数据和迁移授权数据都是KEYAUTH数据结构”(见6.37);

——删除了“B5 F8 09 22 C4 F2 64 08 00 00 00 7D 7F A7 03 D9 04 60 34 F7 4A 8F 79 79 E1 BB 1C 88 A3 77 73 D2 75 9B 56 EA F3 1D 9F F0 C2 03 0F EC ”(见6.42);

——增加了“(参考文献[7])”(见6.46,6.47,6.48);

——修改了“也可以是其他PCR,具体参见GM/T0011—2012中的描述”(见6.56);

——修改了“也可以是其他PCR,具体参见GM/T0011—2012中的描述”(见6.59)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中国科学院软件研究所、国家密码管理局商用密码检测中心、国民技术股份有限公司、同方股份有限公司、首都师范大学信息工程学院、重庆邮电大学。

本文件主要起草人：秦宇、张倩颖、赵世军、冯伟、刘敬彬、周星锦、吴秋兴、李国友、吕春梅、罗鹏、初晓博、刘鑫、宁晓魁、郑必可、李茜、刘韧、李昊。

本文件代替了 GM/T 0013—2012。

GM/T 0013—2021 的历次版本发布情况为：

2012 年首次发布为 GM/T 0013—2012，本次为第一次修订。

引　言

为了推动我国可信计算技术的发展，国家密码管理局于2012年发布了GM/T 0011—2012《可信计算　可信密码支撑平台功能与接口规范》，用以指导我国相关可信计算产品开发和应用。然而，不同厂商生产的产品规格和技术指标可能有所差别，因此必须对相关产品进行完整的符合性测试，以保证产品之间的兼容性。

本文件凡涉及密码算法相关内容，按照国家有关法规实施。

可信计算　可信密码模块接口符合性测试规范

1　范围

本文件以《可信计算　可信密码支撑平台功能与接口规范》(GM/T 0011—2012)为基础,规范了可信密码模块的接口命令测试向量、测试方法与测试脚本。

本文件仅适用于可信密码模块的符合性测试,不能取代其安全性检查。可信密码模块的安全性检测需要按照国家密码管理局的其他相关标准来进行。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 5271.8—2001　信息系统　词汇　第8部分:安全

GB/T 16264.8—2005　信息技术　开放系统互连　目录　第8部分:公钥和属性证书框架

GB 17859—1999　计算机信息系统安全保护等级划分准则

GB/T 18336(所有部分)　信息技术　安全技术　信息技术安全性评估准则

GB/T 32905　信息安全技术　SM3密码杂凑算法

GB/T 32907　信息安全技术　SM4分组密码算法

GB/T 32918(所有部分)信息安全技术　SM2椭圆曲线公钥密码算法

GM/T 0011—2012　可信计算　可信密码支撑平台功能与接口规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

可信计算平台　trusted computing platform

构建在计算系统中,用于实现可信计算功能的支撑系统。

3.2

可信密码模块　trusted cryptography module;TCM

可信计算平台的硬件模块,为可信计算平台提供密码运算功能,具有受保护的存储空间。

3.3

平台配置寄存器　platform configuration register;PCR

可信密码模块内部用于存储平台完整性度量值的存储单元。

3.4

TCM背书密钥　TCM endorsement key;EK

可信密码模块的初始密钥。